

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2006-244044

(P2006-244044A)

(43) 公開日 平成18年9月14日(2006.9.14)

(51) Int.Cl.

G06F 3/12 (2006.01)  
G06K 17/00 (2006.01)

F 1

G06F 3/12  
G06F 3/12  
G06K 17/00  
G06K 17/00

C  
K  
F  
L

テーマコード(参考)

5B021  
5B058

審査請求 未請求 請求項の数 9 O L (全 12 頁)

(21) 出願番号  
(22) 出願日

特願2005-57641 (P2005-57641)  
平成17年3月2日 (2005.3.2)

(71) 出願人 000005496  
富士ゼロックス株式会社  
東京都港区赤坂二丁目17番22号  
(74) 代理人 100071054  
弁理士 木村 高久  
(72) 発明者 秋中 孝則  
神奈川県川崎市高津区坂戸3丁目2番1号  
K S P R & D ビジネスパークビル  
富士ゼロックス株式会社内  
F ターム(参考) 5B021 AA04 CC05 LL06 NN18 NN19  
QQ01 QQ07  
5B058 CA15 KA31 YA20

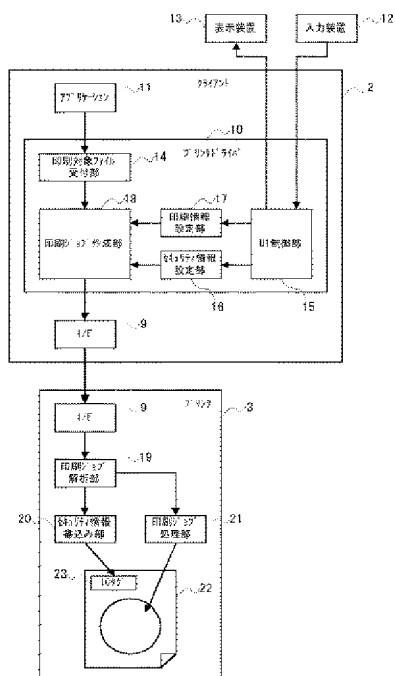
(54) 【発明の名称】文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタ

(57) 【要約】

【課題】印刷物を紙1枚単位で持ち出しの制限を実施することで、文書等のセキュリティを高めることが可能な文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタを提供する。

【解決手段】入力装置によりセキュリティ情報および印刷情報を入力し、印刷ジョブ作成部はアプリケーションからの印刷対象ファイルに基づいて印刷ジョブを作成し、作成した印刷ジョブに対し、セキュリティ情報指定部がセキュリティ情報を設定するとともに印刷情報設定部が印刷情報を設定し、印刷ジョブをプリンタに送信し、プリンタの印刷ジョブ解析部は印刷ジョブを解析し、印刷ジョブ処理部は印刷情報を従って印刷対象ファイルの画像を用紙上に形成し、セキュリティ情報書き込み部はセキュリティ情報を用紙に埋め込まれたICタグに書き込む。

【選択図】図2



**【特許請求の範囲】****【請求項1】**

クライアント装置からの印刷ジョブに基づき、プリンタが印刷した文書の文書持出制限システムにおいて、

前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成する処理と、

前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定する処理と、

該設定した印刷ジョブを前記プリンタに送信する処理と

をクライアント装置に動作させるプリンタドライバと、

前記クライアント装置から受信した印刷ジョブを解析する印刷ジョブ解析手段と、

前記印刷ジョブ解析手段で解析した印刷ジョブに設定されたセキュリティ情報を、前記用紙に付加されたICタグに書き込むセキュリティ情報書き込み手段と、

前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを前記用紙に形成する印刷ジョブ処理手段と

を具備するプリンタと

を具備することを特徴とする文書持出制限システム。

**【請求項2】**

前記用紙に付加されたICタグに書き込まれたセキュリティ情報を読み込むセキュリティ情報読込手段と、

前記セキュリティ情報読込手段で読み込んだセキュリティ情報に基づき、前記用紙が前記持出可能範囲への持出が許可されているか否か判定する判定手段と

を具備し、前記持出可能範囲の境界に設置された検出器

を更に具備することを特徴とする請求項1記載の文書持出制限システム。

**【請求項3】**

前記プリンタドライバは、

前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する処理

をクライアント装置に動作させることを特徴とする請求項1記載の文書持出制限システム。

**【請求項4】**

クライアント装置からの印刷ジョブに基づき、プリンタが印刷した文書の文書持出制限方法において、

前記クライアント装置のプリンタドライバは、

前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成し、

前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定し、

該設定した印刷ジョブを前記プリンタに送信し、

前記プリンタは、

前記クライアント装置から受信した印刷ジョブを解析し、

該解析した印刷ジョブに設定されたセキュリティ情報を、前記用紙に付加されたICタグに書き込み、

該解析した印刷ジョブに含まれる印刷データを前記用紙に形成する

ことを特徴とする文書持出制限方法。

**【請求項5】**

前記持出可能範囲の境界に設置された検出器は、

前記用紙に付加されたICタグに書き込まれたセキュリティ情報を読み込み、

該読み込んだセキュリティ情報に基づき、前記用紙が前記持出可能範囲への持出が許可されているか否か判定する

ことを特徴とする請求項4記載の文書持出制限方法。

**【請求項6】**

前記プリンタドライバは、  
前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する  
ことを特徴とする請求項4記載の文書持出制限方法。

**【請求項7】**

プリンタに送信する印刷ジョブを作成するクライアント装置にインストールされたプリンタドライバにおいて  
前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成する処理と、  
前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定する処理と、  
該設定した印刷ジョブを前記プリンタに送信する処理と  
をクライアント装置に動作させることを特徴とするプリンタドライバ。

**【請求項8】**

前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する処理  
をクライアント装置に動作させることを特徴とする請求項7記載のプリンタドライバ。

**【請求項9】**

クライアント装置と接続するプリンタにおいて、  
前記クライアント装置から受信した印刷ジョブを解析する印刷ジョブ解析手段と、  
前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を、該用紙に付加されたICタグに書き込むセキュリティ情報書き込み手段と、  
前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを前記用紙に形成する印刷ジョブ処理手段と  
を具備することを特徴とするプリンタ。

**【発明の詳細な説明】****【技術分野】****【0001】**

本発明は、文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタに関し、特に、用紙に埋め込まれたICタグの情報に基づいて文書の持ち出しを制限する文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタに関するもの。

**【背景技術】****【0002】**

近年、スーパーマーケット、百貨店、小売店等の店舗における商品の万引きまたは盗難を防止する目的で、それら商品の包装材に盗難防止用のICタグ等が取り付けられことが多いとなっている。

**【0003】**

この盗難防止用のICタグは通常カード状を呈し、例えば、特定の周波数の電磁波に感応し、この電磁波と同一または異なる周波数の電磁波を発信し、若しくは磁性体により電磁場等の所定の場の変化を店舗の出口等で検知することにより万引きまたは盗難を防止するものである。

**【0004】**

例えば、ICタグを利用して、ホテル、マンション等の内部を複数のエリアに分割された建物において、各エリアへの出入り管理を自動的に行うとともに、出入りにより各エリアに装備された照明施設、空調施設等を自動的に作動／停止することができる特定エリアへの出入りによるサービス提供システムがある（例えば、特許文献1参照。）。

**【0005】**

また、例えば、ICタグを利用して、書籍、雑誌等の包装材料に情報の読み書き可能なICタグを備え、この包装材料と書籍、雑誌等を一体にすることにより、物流管理、返本管

理、万引き防止等の機能を備えることができる書籍、雑誌等の包装材料がある（例えば、特許文献2参照。）。

【特許文献1】特開平5-263558号公報

【特許文献2】特開2002-326476号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかし、上記特許文献2に記載の技術では、紙1枚単位の持ち出しを制限することは困難である。

【0007】

そこで、本発明は、印刷物を紙1枚単位で持ち出しの制限を実施することで、文書等のセキュリティを高めることが可能な文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタを提供することを目的とする。

【課題を解決するための手段】

【0008】

上記目的を達成するため、請求項1の発明は、クライアント装置からの印刷ジョブに基づき、プリンタが印刷した文書の文書持出制限システムにおいて、前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成する処理と、前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定する処理と、該設定した印刷ジョブを前記プリンタに送信する処理とをクライアント装置に動作させるプリンタドライバと、前記クライアント装置から受信した印刷ジョブを解析する印刷ジョブ解析手段と、前記印刷ジョブ解析手段で解析した印刷ジョブに設定されたセキュリティ情報を、前記用紙に付加されたICタグに書き込むセキュリティ情報書き込み手段と、前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを前記用紙に形成する印刷ジョブ処理手段とを具備するプリンタとを具備することを特徴とする。

【0009】

また、請求項2の発明は、請求項1の発明において、前記用紙に付加されたICタグに書き込まれたセキュリティ情報を読み込むセキュリティ情報読込手段と、前記セキュリティ情報読込手段で読み込んだセキュリティ情報に基づき、前記用紙が前記持出可能範囲への持出が許可されているか否か判定する判定手段とを具備し、前記持出可能範囲の境界に設置された検出器を更に具備することを特徴とする。

【0010】

また、請求項3の発明は、請求項1の発明において、前記プリンタドライバは、前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する処理をクライアント装置に動作させることを特徴とする。

【0011】

また、請求項4の発明は、クライアント装置からの印刷ジョブに基づき、プリンタが印刷した文書の文書持出制限方法において、前記クライアント装置のプリンタドライバは、前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成し、前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定し、該設定した印刷ジョブを前記プリンタに送信し、前記プリンタは、前記クライアント装置から受信した印刷ジョブを解析し、該解析した印刷ジョブに設定されたセキュリティ情報を、前記用紙に付加されたICタグに書き込み、該解析した印刷ジョブに含まれる印刷データを前記用紙に形成することを特徴とする。

【0012】

また、請求項5の発明は、請求項4の発明において、前記持出可能範囲の境界に設置された検出器は、前記用紙に付加されたICタグに書き込まれたセキュリティ情報を読み込み、該読み込んだセキュリティ情報に基づき、前記用紙が前記持出可能範囲への持出が許可されているか否か判定することを特徴とする。

**【0013】**

また、請求項6の発明は、請求項4の発明において、前記プリンタドライバは、前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定することを特徴とする。

**【0014】**

また、請求項7の発明は、プリンタに送信する印刷ジョブを作成するクライアント装置にインストールされたプリンタドライバにおいて前記プリンタで印刷する印刷データに基づき、印刷ジョブを作成する処理と、前記プリンタで前記印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を前記印刷ジョブに設定する処理と、該設定した印刷ジョブを前記プリンタに送信する処理とをクライアント装置に動作させることを特徴とする。

**【0015】**

また、請求項8の発明は、請求項7の発明において、前記プリンタで前記印刷データを形成した用紙を持出可能範囲外への持出を許可するセキュリティ情報を前記印刷ジョブに設定する処理をクライアント装置に動作させることを特徴とする。

**【0016】**

また、請求項9の発明は、クライアント装置と接続するプリンタにおいて、前記クライアント装置から受信した印刷ジョブを解析する印刷ジョブ解析手段と、前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを形成した用紙毎の持出可能範囲を指定したセキュリティ情報を、該用紙に付加されたICタグに書き込むセキュリティ情報書き込み手段と、前記印刷ジョブ解析手段で解析した印刷ジョブに含まれる印刷データを前記用紙に形成する印刷ジョブ処理手段とを具備することを特徴とする。

**【発明の効果】****【0017】**

本発明によれば、印刷物に対して、紙1枚単位で建物または建物のフロア毎にセキュリティを管理することが可能になるという効果を奏する。

**【発明を実施するための最良の形態】****【0018】**

以下、本発明に係る文書持出制限システム、文書持出制限方法、プリンタドライバおよびプリンタの実施の形態について添付図面を参照して詳細に説明する。なお、実施の形態として、ネットワークを介して本発明に係るプリンタとPC[Personal Computer]等のクライアントとが接続し、クライアントに本発明に係るプリンタドライバがインストールされている構成を一例にして説明する。

**【0019】**

図1は、本発明を適用した文書持出制限システム1の全体構成の一例を示すブロック図である。

**【0020】**

図1に示すように、クライアント2とプリンタ3とがネットワーク4を介して接続している。なお、クライアント2-プリンタ3間をネットワーク4接続に限定する必要は無く、例えば、USB等のローカル接続の構成も適用可能である。

**【0021】**

図1に示すように、クライアント2は、CPU5、ROM6、RAM7、HD8、I/F9を備して構成される。

**【0022】**

CPU[Central Processing Unit]5は、基本ソフトウェアであるオペレーティングシステム(以後、OSと称する)に基づいてクライアント2本体のシーケンス制御を行なう。

**【0023】**

ROM[Read Only Memory]6は、クライアント2の起動時に実行されるプログラム等を記録する。

**【0024】**

R A M [Random Access Memory] 7は、プログラムの実行に必要なワークエリアのバッファエリアとして利用される。

**【0025】**

H D [Hard Disk] 8は、O S、アプリケーションプログラム（以後、アプリケーションと称する）、プリンタドライバ、各種データ等を格納する。

**【0026】**

I / F [Interface] 9は、ネットワーク4上のプリンタ3等の装置との間で各種データの送受信を行う。

**【0027】**

図2は、本発明に係るプリンタドライバ10およびプリンタ3の機能的な構成の一例を示すブロック図である。

**【0028】**

図2に示すように、クライアント2には本発明に係るプリンタドライバ10、および各種のアプリケーション11がインストールされ、これらは、図示しないO Sの制御下で、O Sの機能を利用して各種処理を実行する。また、P Cにはキーボードまたはマウス等の入力装置12、ディスプレイ等の表示装置13が接続されている。なお、前述したクライアント2に関する構成部以外の本発明と無関係な構成部についての説明は省略する。

**【0029】**

次に、プリンタドライバ10の機能的な構成について説明する。

**【0030】**

図2に示すように、プリンタドライバ10は、その機能として、印刷対象ファイル受付部14、U I制御部15、セキュリティ情報設定部16、印刷情報設定部17、印刷ジョブ作成部18から構成される。

**【0031】**

印刷対象ファイル受付部14は、アプリケーション11から出力される文書、グラフィックまたは画像等の印刷対象ファイルを受け付ける処理を行う。

**【0032】**

U I制御部15は、表示装置13に表示するプリンタドライバU I画面の表示制御の処理、入力装置12から入力された印刷対象ファイルの印刷に関する印刷情報、用紙に埋め込まれたI Cタグに書き込むセキュリティ情報等を受け付ける処理等を行う。

**【0033】**

セキュリティ情報設定部16は、U I制御部15で受け付けたセキュリティ情報を、印刷ジョブ作成部18で作成する印刷ジョブに設定する処理を行う。ここで、セキュリティ情報とは、例えば、セキュリティの有無、持出可能範囲等の用紙持出制限を示す情報であり、印刷対象ファイルが複数の用紙で出力される場合は、各用紙毎にセキュリティ情報を設定することができる。例えば、1ページ目は持ち出しを許可し、2ページ目は事業所外への持ち出しを禁止し、3ページ目は建物外への持ち出しを禁止し、4ページ目はフロア外への持ち出しを禁止する、というように各ページ毎に持ち出し制限を設定することができる。

**【0034】**

印刷情報設定部17は、U I制御部15で受け付けた印刷情報を、印刷ジョブ作成部18で作成する印刷ジョブに設定する処理を行う。

**【0035】**

印刷ジョブ作成部18は、印刷対象ファイル受付部14で受け付けた印刷対象ファイル、セキュリティ情報設定部16で設定したセキュリティ情報、および印刷情報設定部17で設定した印刷情報に基づいて印刷ジョブを作成する処理を行い、作成した印刷ジョブをI / F 9を介してプリンタに送信する処理を行う。

**【0036】**

次に、プリンタ3の機能的な構成について説明する。

**【0037】**

図2に示すように、プリンタ3は、I/F9、印刷ジョブ解析部19、セキュリティ情報書込み部20、印刷ジョブ処理部21を具備して構成される。なお、前述したプリンタ3に関する構成部以外の本発明と無関係な構成部についての説明は省略する。

**【0038】**

I/F9は、ネットワーク4上のクライアント2等の装置との間で各種データの送受信を行う。

**【0039】**

印刷ジョブ解析部19は、クライアント2から受信した印刷ジョブを解析する処理を行う。

**【0040】**

セキュリティ情報書込み部20は、印刷ジョブ解析部19で解析した印刷ジョブに含まれるセキュリティ情報を、用紙22に埋め込まれたICタグ23に書き込む処理を行う。

**【0041】**

印刷ジョブ処理部21は、印刷ジョブ解析部19で解析した印刷ジョブに含まれる印刷対象ファイルを印刷情報に従って画像に展開し、展開した画像を用紙22上に形成する印字処理を行う。

**【0042】**

次に、印刷用紙にセキュリティ情報を書き込む際に行われるクライアント2およびプリンタ3の機能的な動作について図2を参照して説明する。

**【0043】**

ユーザが入力装置12によりセキュリティ情報および印刷情報を入力し、クライアント2にインストールされたプリンタドライバ10のUI制御部15は入力装置12から入力されたセキュリティ情報および印刷情報を受け付け、セキュリティ情報をセキュリティ情報設定部16に渡すとともに、印刷情報を印刷情報設定部17に渡す。

**【0044】**

印刷対象ファイル受付部14はアプリケーション11から印刷対象ファイルを受け付けると、受け付けた印刷対象ファイルを印刷ジョブ作成部18に渡し、印刷ジョブ作成部18は印刷対象ファイルを受け取ると、受け取った印刷対象ファイルに基づいて印刷ジョブを作成し、作成した印刷ジョブに対し、セキュリティ情報指定部16がセキュリティ情報を設定するとともに印刷情報設定部17が印刷情報を設定し、印刷ジョブ作成部18は印刷ジョブをI/F9を介してプリンタ3に送信する。

**【0045】**

プリンタ3の印刷ジョブ解析部19はI/F9を介して受信した印刷ジョブを解析し、印刷ジョブに含まれたセキュリティ情報をセキュリティ情報書込み部20に渡し、印刷ジョブに含まれた印刷対象ファイルおよび印刷情報を印刷ジョブ処理部21に渡し、印刷ジョブ処理部21は印刷対象ファイルおよび印刷情報を受け取ると、印刷情報に従って印刷対象ファイルの画像を用紙22上に形成し、セキュリティ情報書込み部20はセキュリティ情報を用紙22に埋め込まれたICタグ23に書き込む。

**【0046】**

図3は、用紙22に埋め込まれたICタグ23に書き込まれたセキュリティ情報を検出する検出器24の機能的な構成の一例を示すブロック図である。

**【0047】**

図3に示すように、検出器24は、所定の範囲に進入した用紙22に埋め込まれたICタグ23に書き込まれたセキュリティ情報を読み込むセキュリティ情報読込部25、この検出器24に設定された持出制限の情報を格納する制限情報格納部26、セキュリティ情報読込部25が読み込んだセキュリティ情報と、制限情報格納部26に格納されている持出制限の情報を比較することにより用紙の持出許可／持出禁止を判定する判定部27を具備して構成される。なお、判定部27で持出禁止と判定した場合は警告出力装置28が警告音等を出力し、用紙22を持ち出そうとするユーザに対して注意を促す。

**【0048】**

次に、クライアントのプリンタドライバで行われる印刷用紙にセキュリティ情報を書き込む印刷ジョブを作成するための処理手順について図4に示すフローチャートを参照して説明する。

**【0049】**

アプリケーションから印刷対象ファイルを受け付け（ステップS401）、受け付けた印刷対象ファイルに基づいて印刷ジョブを作成し（ステップS402）、入力されたセキュリティ情報を受け付け（ステップS403）、受け付けたセキュリティ情報を印刷ジョブに設定し（ステップS404）、印刷ジョブをプリンタに送信し（ステップS405）、印刷ジョブを作成するための処理手順を終了する。

**【0050】**

次に、プリンタで行われる印刷用紙に埋め込まれたICタグにセキュリティ情報を書き込むための処理手順について図5に示すフローチャートを参照して説明する。

**【0051】**

クライアントから印刷ジョブを受信し（ステップS501）、受信した印刷ジョブを解析し（ステップS502）、印刷ページを表す「n」を「0」に設定し（ステップS503）、「n」に「1」を加算し（ステップS504）、印刷ジョブに含まれたnページ目の画像を用紙上に形成し（ステップS505）、印刷ジョブに含まれたセキュリティ情報を用紙に埋め込まれたICタグに書き込み（ステップS506）、nページ目が最終ページではない場合（ステップS507でNO）、ステップS504に戻り、また、nページ目が最終ページである場合（ステップS507でYES）、ICタグにセキュリティ情報を書き込むための処理手順を終了する。

**【0052】**

次に、検出器で行われるICタグから読み込んだセキュリティ情報に基づいて用紙持ち出しの許可／禁止を判定するための処理手順について図6に示すフローチャートを参照して説明する。

**【0053】**

所定の範囲に進入した用紙に埋め込まれたICタグからセキュリティ情報を読み込み（ステップS601）、セキュリティ情報と制限情報に基づいて持出制限を判定し（ステップS602）、持出禁止の場合（ステップS603でYES）、ステップS604に進み、また、持出許可の場合（ステップS603でNO）、持出の許可／禁止を判定するための処理手順を終了する。

**【0054】**

持出禁止の場合（ステップS603でYES）、警告出力装置に警告を出力するように指示し（ステップS604）、持出の許可／禁止を判定するための処理手順を終了する。

**【0055】**

図7は、本発明に係る用紙持出制限方法の具体例を示す図である。

**【0056】**

図7に示すように、複数の用紙で構成されている文書があり、各用紙毎にICタグが埋め込まれ、そのICタグには、「任意の範囲（例えば、部屋、フロア、建物等）の中での異動は可能」、「その任意の範囲外への持出は禁止」というセキュリティ情報が書き込まれ、その任意の範囲外へ出る出口には検出器および警告出力装置が設置されている。

**【0057】**

従って、その文書のうち1枚の用紙を人が範囲外に持ち出そうとしても、出口に設置された検出器が、持ち出そうとする1枚の用紙のICタグに書き込まれたセキュリティ情報に基づいてその用紙が持出禁止の用紙であることを判定し、警告出力装置から警告音等が出力される。

**【0058】**

このように、用紙1枚単位で持出許可／禁止の管理を行うことで、例えば、スーパーマーケット、百貨店、小売店等の店舗における商品の万引きまたは盗難を防止する以外にも

、図書館の本のページを破いて持ち出す行為、会社に保管された文書の中から機密情報が記載された用紙のみを持ち出す行為等も防止することが可能になる。

【0059】

また、図8に示すように、特別な事情があって任意の範囲外に用紙を持ち出さなければならぬ場合、その用紙の持出を許可する情報をI Cタグに書き込んだ持出許可用紙29を、本発明に係るプリンタドライバおよびプリンタで印刷し、その持出許可用紙29と持出用紙とと一緒に持つことで、検出器が持出用紙の持出を許可し、警告出力装置から警告音等が出力されないような構成も可能である。

【0060】

なお、本発明の実施の形態として、クライアントにインストールされたプリンタドライバが印刷ジョブにセキュリティ情報を設定する構成を一例に説明したが、本発明はこのような構成に限定する必要は無く、例えば、プリンタのコントロールパネル等でセキュリティ情報を入力し、プリンタがそのセキュリティ情報を用紙のI Cタグに書き込む構成も適応可能であり、更に、このようなセキュリティ情報を書き込むことが可能なコピー機も適応可能である。

【図面の簡単な説明】

【0061】

【図1】本発明を適用した文書持出制限システムの全体構成の一例を示すブロック図である。

【図2】本発明に係るプリンタドライバおよびプリンタの機能的な構成の一例を示すブロック図である。

【図3】用紙に埋め込まれたI Cタグに書き込まれたセキュリティ情報を検出する検出器の機能的な構成の一例を示すブロック図である。

【図4】クライアントのプリンタドライバで行われる印刷用紙にセキュリティ情報を書き込む印刷ジョブを作成するための処理手順を示すフローチャートである。

【図5】プリンタで行われる印刷用紙に埋め込まれたI Cタグにセキュリティ情報を書き込むための処理手順を示すフローチャートである。

【図6】検出器で行われるI Cタグから読み込んだセキュリティ情報に基づいて用紙持出しの許可／禁止を判定するための処理手順を示すフローチャートである。

【図7】本発明に係る用紙持出制限方法の具体例を示す図である。

【図8】持出許可用紙を説明する図である。

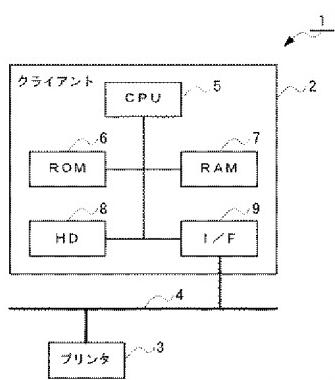
【符号の説明】

【0062】

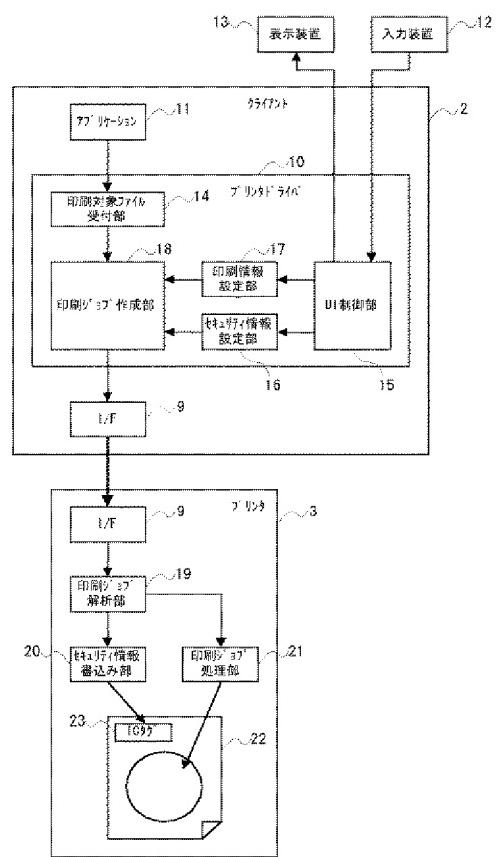
- 1 文書持出制限システム
- 2 クライアント
- 3 プリンタ
- 4 ネットワーク
- 5 C P U
- 6 R O M
- 7 R A M
- 8 H D
- 9 I / F
- 10 プリンタドライバ
- 11 アプリケーション
- 12 入力装置
- 13 表示装置
- 14 印刷対象ファイル受付部
- 15 U I 制御部
- 16 セキュリティ情報設定部
- 17 印刷情報設定部

- 1 8 印刷ジョブ作成部
- 1 9 印刷ジョブ解析部
- 2 0 セキュリティ情報書き込み部
- 2 1 印刷ジョブ処理部
- 2 2 用紙
- 2 3 I C タグ
- 2 4 検出器
- 2 5 セキュリティ情報読み込部
- 2 6 制限情報格納部
- 2 7 判定部
- 2 8 警告出力装置
- 2 9 持出許可用紙

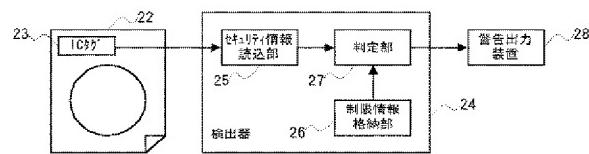
【図1】



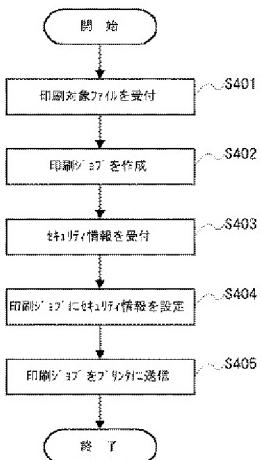
【図2】



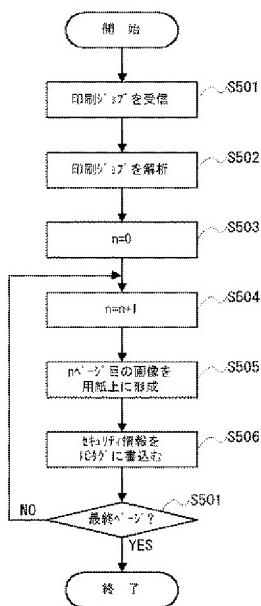
【図3】



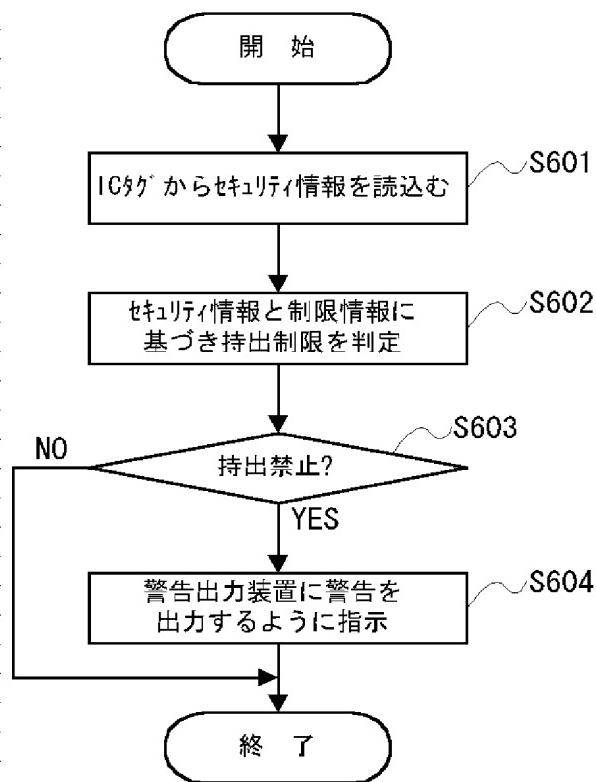
【図4】



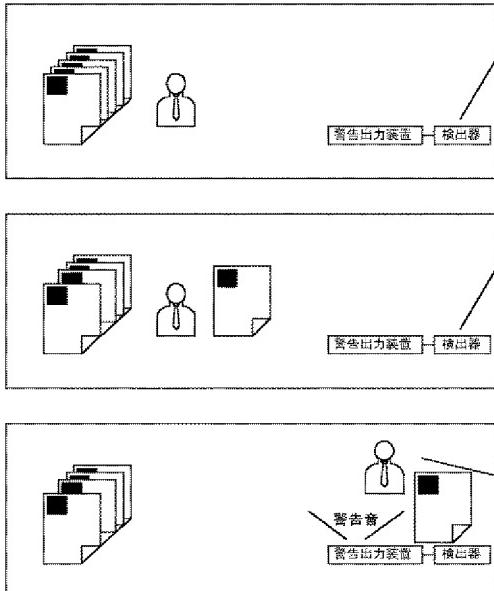
【図5】



【図6】



【図7】



【図8】

